DiSign

Objective

Explore authentication of documents by digitally signing a file and subsequently authenticating the document by verifying the signature.

User needs and requirements

Id	Need/Requirement
1	The utility shall support generating a signature file containing the digital signature of a given file.
2	Digitally signing a file should use a private key in conformance with X509.
3	The utility shall support authenticating a file against a digital signature file.
4	Authenticating a file should use the public key (of the private/public key pair).
5	The file and its signature file should be combined into a password protected container file. (zip/tar are potential choices).

User wants

The following will enhance the appeal of the tool.

Id	Wants
1	The utility shall support the generation of a public, private key pair to be stored in an X509 compatible form.
2	Conceptually this should be an extension of the “password” projectlet.

Example usage